INFO-HAMS Digest Sat, 23 Dec 89 Volume 89 : Issue 1062

Today's Topics:

ARRL and tx/rx mods
Interception of E-Mail by spies
Packet compression, what issue?
Profanity on rec.ham-radio
Strong language and retansmission.

Date: 23 Dec 89 14:44:59 GMT
From: asuvax!anasaz!john@handies.ucar.edu (John Moore)
Subject: ARRL and tx/rx mods
Message-ID: <1069@anasaz.UUCP>

In article <10710@attctc.Dallas.TX.US> sampson@attctc.Dallas.TX.US (Steve Sampson) writes:
]In article <7880101@hpfcdc.HP.COM>, perry@hpfcdc.HP.COM (Perry Scott) writes:
]> I've been told that most military
]> bands do not need the type acceptance.
]>
]> Funny how the government treats itself and commercial interests differently.
]>
]> Perry Scott
]> KF0CA
]
]The military/government agencies have special calibration and repair facilities
]where civilians usually use a radio until it dies. By ensuring that all radios
]go through a cal check on a periodic schedule, the type acceptance is a
]taxpayer waste.

Gee, I use amateur equipment on military bands all the time, and no one has ever come by to cal check it! The Civil Air Patrol uses military frequencies. Also, in Arizona, the national guard operates on 2 meter FM just outside the ham bands. Standard equipment consists of Kenwood ham radios. The national guard communications auxilliary, called Broadway Consumer, is composed of all hams and uses their own equipment on the same frequencies.

In fact, I am one of those with a legitimate reason to use ham equipment out of band - for CAP and Broadway Consumer.

--
John Moore (NJ7E) mcdphx!anasaz!john asuvax!anasaz!john
(602) 951-9326 (day or eve) long palladium, short petroleum
7525 Clearwater Pkwy, Scottsdale, AZ 85253
Freedom and Communism are incompatable.

Date: 23 Dec 89 18:38:59 GMT
From: nuchat!moray!siswat!buck@uunet.uu.net (A. Lester Buck)
Subject: Interception of E-Mail by spies
Message-ID: <489@siswat.UUCP>

In article <5926@alvin.mcnc.org>, spl@mcnc.org (Steve Lamont) writes:
< In article <34958@grapevine.uucp> koreth@panarthea.ebay.sun.com (Steven Grimm)
writes:
< >Anyone who knows anything about mail routing can safely laugh at the
< >original message. (a) The NSA or whoever would have to have a tap,
< >running continuously, on every inter-computer connection, which (with
< >UUCP) means every phone line, in the country. They'd have to transmit
< >all the mail messages back to some central location. I wish I was selling
< >them the disks they'd need to hold a day's worth of E-mail traffic.
<
< ... any idea how many Crays NSA has? The answer is "many." They now admit to
< having at least one of "each" -- that is, at least one X-MP, one Cray-2, and
< one Y-MP, although my primary sources indicate that there are many more. All
< you have to do is to count the missing serial numbers. They certainly have a
< sufficient amount of disk space -- my primary source considers our 40 GBytes
< of rotating storage in our installation "tiny." I'll leave you to draw your
< own conclusions.
<
< As far as shoving bits from one places to another, conversations with my
< primary sources indicate that the NSA is on the forefront of high speed
< networking.
<

I had an interview with NSA at Fort Meade for a job doing applied physics
research in 1981. The guy who was my host was doing research on E-beam
storage because optical disks did not have high enough density for their
needs. The Library of Congress was referred to as a drop in the bit bucket
compared to their daily data collection. Remember the primary mission of
the NSA is to analyze all electronic communications intercepted by the
entire U.S. military around the world. These interceptions are typically a
very high bandwith magnetic tape with the raw signal recorded. The
processing power to munch this type of data is hardly going to build up a
sweat looking through email. Listening in on international telephone links
for key words is only a bit harder on this scale.

But so what? Anything important is certainly encrypted these days.

--
A. Lester Buck   buck@siswat.lonestar.org ...!texbell!moray!siswat!buck

---

Date: 24 Dec 89 01:40:19 GMT
From: zaphod.mps.ohio-state.edu!brutus.cs.uiuc.edu!ux1.cso.uiuc.edu!
ux1.cso.uiuc.edu!phil@tut.cis.ohio-state.edu
Subject: Packet compression, what issue?
Message-ID: <30500337@ux1.cso.uiuc.edu>

(This posting contains long FCC rule quotes and analysis)

>From: Perry Scott KF0CA
> Perhaps we can conform to the spirit of the law by adopting public conventions
> for compressed files. The "Z" convention for Lempil-Ziv UNIX(tm) files makes
> the "cipher" readable by anyone.

Yes, I am sure we can. Read on.

>From: Perry Scott KF0CA
> I recall passages in the FCC regs about having the key available at your
> station for decrypting, and making it available upon request from the FCC.
> Maybe that was back in 1975 and the rules have changed.

You should have a copy of the new rules. I'll supply a copy of the sections
that affects this discussion:

[bracketed sections by ka9wgn, skipped section for brevity, read your copy]
begin FCC rule quote {
97.307 Emission standards.
    (a)-(e) ...[various emission standards rules skipped]
    (f) The following standards and limitations apply to transmission on the
  frequencies specified in 97.305(c) of this Part.
[see 97.305(c) for which paragraphs apply to which subbands]
[be sure to see Sept 27 corrections as June 20 version had many errors]
    (1) ...[section on angle modulation skipped]
    (2) [note this paragraph does not apply (due to 97.305(c)) to RTTY and
  data emissions, except on 160m] No non-phone emission shall exceed the
  bandwidth of a communications quality phone emission of the same modulation
  type. The total bandwidth of an independent sideband emission (having B as
  the first symbol), or a multiplexed image and phone emission, shall not
  exceed that of a communications quality A3E emission.
    (3) [160-12m] Only a RTTY or date [note, "date" spelling error has NOT been
  corrected by FCC] emission using a specified digital code listed in 97.309(a)
  of this Part may be transmitted. The symbol rate must not exceed 300 bauds,
  or for frequency-shift keying, the frequency shift between mark and space
  must not exceed 1 kHz.
    (4) [28.0-28.3 Mhz] Only a RTTY or data emission using a specified digital
  code listed in 97.309(a) of this Part may be transmitted. The symbol rate
  must not exceed 1200 baunds, or for frequency-shift keying, the frequency

shift between mark and space must not exceed 1 kHz.

(5) [6m,2m][125cm was erroneously applied in the June 20 version, but has been deleted (see 6) in the Sept 27 version] A RTTY, data or multiplexed emission using a specified digital code listed in 97.309(a) of this Part may be transmitted. The symbol rate must not exceed 19.6 [not 19.2] kilobauds. A RTTY, data or multiplexed emission using an unspecified digital code under the limitations listed in 97.309(b) of this Part may also be transmitted. The authorized bandwidth is 20 kHz.

(6) [125cm,70cm] A RTTY, data or multiplexed emission using a specified digital code listed in 97.309(a) of this Part may be transmitted. The symbol rate must not exceed 56 kilobauds. A RTTY, data or multiplexed emission using an unspecified digital code under the limitations listed in 97.309(b) of this Part also may be transmitted. The authorized bandwidth is 100 kHz.

(7) [33cm and shorter] A RTTY, data or multiplexed emission using a specified digital code listed in 97.309(a) of this Part or an unspecified digital code under the limitations listed in 97.309(b) of this Part may be transmitted.

97.309 RTTY and digital emission codes.

(a)(1)-(3) ...[sections listing specific codes skipped]

(b) Where authorized by 97.305(c) [authorized emission types] and 97.307(f) [bandwidth and baudrate limitations] of this Part, a station may transmit a RTTY or data emission using an unspecified digital code, except to a station in a country with which the United States does not have an agreement permitting the code to be used. RTTY and data emissions using unspecified digital codes must not be transmitted for the purpose of obscuring the meaning of any communication. When deemed necessary by an EIC to assure compliance with the FCC Rules, a station must:

(1) Cease the transmission using the unspecified digital code;

(2) Restrict transmissions of any digital code to the extent instructed;

(3) Maintain a record, convertible to the original information, of all digital communications transmitted.

} end FCC rule quote

My analysis of this tells me that I can use any code I wish to use provided that:

(1) I use 6 meters and above for the transmission, limit my bandwidth to 20 khz on 6m and 2m and to 100 khz on 125cm and 70cm. If I use one of the codes listed in 97.309(a) w/o the limitations in 97.309(b) then I must adhere to the baudrate limitations of 300 (160-12m), 1200 (10m), 19600 (6m,2m) or 56000 (125cm,70cm) baud unless I operate on 33cm or shorter. I do not need to limit my bandwidth on 33cm or shorter.

(2) I do not use it to communicate with any foreign country with which the United States does not have an actual agreement in place to allow the particular code I want to use. I suppose it might be possible for the US to negotiate an agreement allowing ANY code. There should be a list of such countries and what codes are agreed upon for each.

(3) I may not use the code for the purpose of obscuring the meaning. This certainly includes an cypher for which the algorithm and key are not

publicly known. Also, if I happen to believe that someone is not capable of receiving any certain particular code and I switch to using that code so he cannot copy my transmission, even though it might be a publicly known code, then I have fallen under the "for the purpose of obscuring the meaning" clause. This is a matter of INTENT and brings with it all the legal vagaries associated with proving intent.

(4) The Engineer In Charge can direct any combination of the listed requirements on my station (not me, the operator). The third requirement is to maintain a record of what was transmitted (not just what code was used). I am not required to keep this record unless directed to do so by the EIC. Note that by the LETTER of this rule, the EIC can require such a record of ALL digital communications, not just the ones using an uspecified code. While the spirit is apparent to me to be applied to only unspecified codes, I see this as a minor gap in the rules that needs a bit of touching up (petition for rulemaking?).

Further rule nitpicking suggests to me that (in 97.307(f)(3)-(5) applicable to HF frequencies) that EITHER the baudrate limitation applies OR the frequency-shift limitation applies due to the use of the word "or" in the rule text. Since 97.307(f)(2) does not apply to RTTY and data emissions (except in 160m) according to 97.305(c), apparently no bandwidth limitations apply either. So if I have a high baud rate of one of the specified codes, along with the use of frequency shift keying of 1 khz or less, on HF, then the bandwidth will not matter (as no rule paragraphs apply). I believe we call things like this "loopholes". Another petition?

>From: Perry Scott KF0CA
> I think one of the contributions of Amatuer Radio in this area is to squeeze
> more out of RF data networks. So, it is within our charter to request the
> FCC to relax the cipher rule so it doesn't apply to simple compression for
> transmission purposes.

It seems to me, after reading over the rules rather closely, that they are in fact suitable to begin experimentation. Compression codes such as the LZW code fall under the "unspecified" codes and I find them usable within the limitations of 97.305(c), 97.307(f)(5)-(7) and 97.309(b). That rules out using them on HF.

I also believe that I may use checksum and Forward Error Correction codes, as they do not obscure meanings at all where they do not alter the original data. They may still fall under the definition of "unspecified" codes by the LETTER of the rules, which may worry some regarding their use on HF to enhance the reliability of that spectrum. Another petition for rulemaking could clarify this by allowing the appendage of checking, correcting, and authentication codes to the clear data being sent for all specified (and unspecified) codes.

--Phil Howard, KA9WGN--
<phil@ux1.cso.uiuc.edu>

Date: 23 Dec 89 17:40:53 GMT
From: sun-barr!newstop!texsun!pollux!attctc!sampson@lll-winken.llnl.gov (Steve Sampson)
Subject: Profanity on rec.ham-radio
Message-ID: <10723@attctc.Dallas.TX.US>

In article <1731@cod.NOSC.MIL>, medin@cod.NOSC.MIL (Ted Medin) writes:
> In article <8912220803.AA29003@ucbvax.Berkeley.EDU> 702WFG@SCRVMSYS.BITNET (bill gunshannon) writes:
> >:-(
> >I can think of no time when profanity has added any value to a conversation
> >here or anywhere else.
>
> Amen!

God Damn Right!

Date: 23 Dec 89 17:52:08 GMT
From: sun-barr!newstop!texsun!pollux!attctc!sampson@apple.com (Steve Sampson)
Subject: Strong language and retansmission.
Message-ID: <10724@attctc.Dallas.TX.US>

In article <272@ccop1.ocpt.ccur.com>, wilson@ccop1.ocpt.ccur.com (<wilson>) writes:
> Perhaps. As a child though, I was taught by my father that profanity
> is the mark of an uneducated man. An educated man has a vocabulary that
> is sufficiently large enough to make his feelings known without resorting
> to vulgarity.
>
> I would hope that the amateur community considers itself educated.
>
> Gary Wilson, WB2BOO

I was taught just the opposite, course my father cussed alot. He was college educated, even taught school for awhile until he got a real job. An educated man can use vulgarity to replace a whole paragraph. Never trust a man that doesn't swear, he said. What are you protecting the children from when you censor the mail? Those children that can read already know how to swear. You can't read a good novel without being confronted with a swear word. In short, this conversation sounds like two old Baptist ladies talking about the Catholics. Censorship is vulgar, only Communists and Nazi's approve of it.

End of INFO-HAMS Digest V89 Issue #1062
****